Lab 181

Morris & Opazo

aws re/start

Solución de problemas de una VPC

INTRODUCCIÓN

En este laboratorio, solucionará problemas de configuración de nubes privadas virtuales (VPC) y analizará registros de flujo de VPC.

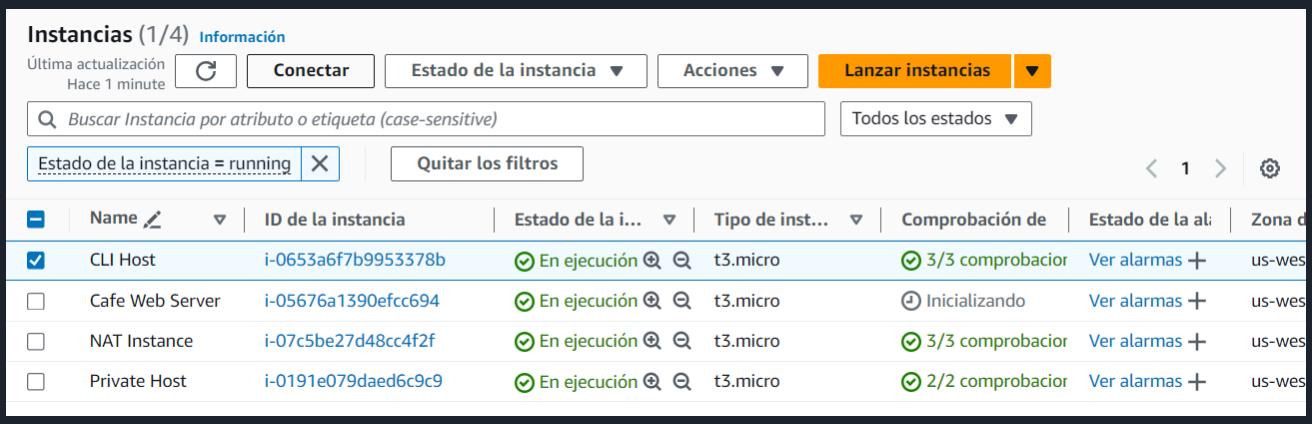
OBJETIVOS

- Crear registros de flujo de VPC.
- Solucionar problemas de configuración de VPC.
- Analizar registros de flujo.

TAREA 1

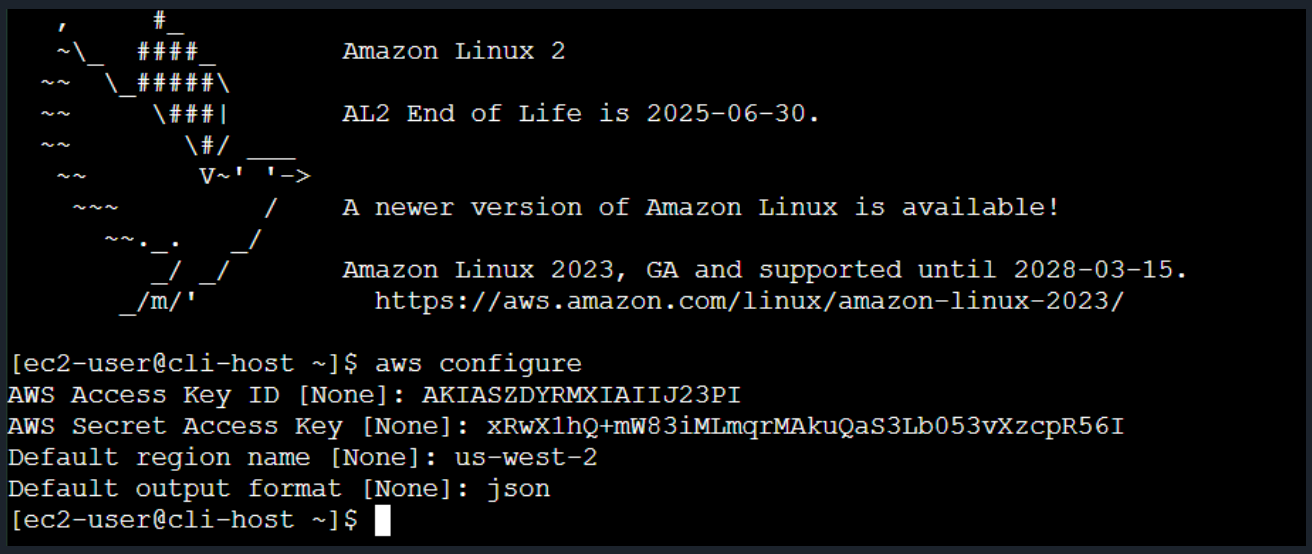
En esta tarea, se utiliza EC2 Instance Connect para conectarse a la instancia del host CLI. Se utiliza esta instancia para ejecutar comandos de la interfaz de línea de comandos de AWS (AWS CLI).

- En la Consola de administración de AWS, en la barra de búsqueda, ingrese y elija EC2 abrir la Consola de administración de EC2.
- En el panel de navegación, seleccione Instancias.
- De la lista de instancias, seleccione la instancia de host CLI.
- Seleccione Conectar.



- En la pestaña Conectar instancia EC2, seleccione Conectar.
- Para configurar el perfil de AWS CLI con credenciales, en la terminal EC2 Instance Connect, ejecute el siguiente comando:

- Siguiendo las indicaciones, copie los siguientes valores que pegó en su editor de texto y péguelos en la ventana de terminal según las instrucciones.



TAREA 2

En esta tarea, se crea un depósito S3 para publicar datos de los registros de flujo de VPC. Luego, se crean registros de flujo de VPC en VPC1 para capturar información sobre el tráfico de IP entre las interfaces de red en VPC1. Luego, los registros de flujo se publican en el depósito S3.

- Para crear el depósito S3 donde se publicarán los registros de flujo, ejecute el siguiente comando. En el comando, reemplace ###### con seis números aleatorios:

```
[ec2-user@cli-host ~]$ aws s3api create-bucket --bucket flowlog123456 --region 'us-west-2' --create-bucket-configuration LocationConstraint='
us-west-2'
{
    "Location": "http://flowlog123456.s3.amazonaws.com/"
}
[ec2-user@cli-host ~]$
```

- Para obtener el ID de VPC para VPC1 para crear registros de flujo de VPC, ejecute el siguiente comando:

```
[ec2-user@cli-host ~]$ aws ec2 describe-vpcs --query 'Vpcs[*].[VpcId,Tags[?Key==`Name`].Value,CidrBlock]' --filters "Name=tag:Name,Values='VP
C1'"
[
    [
        "vpc-00273783f78bba119",
        [
            "VPC1"
        ],
        "10.0.0.0/16"
    ]
]
```

- Para crear registros de flujo de VPC en VPC1, ejecute el siguiente comando. En el comando, reemplace < flowlog###### > con el nombre del depósito de los pasos anteriores y reemplace < vpc-id > con el ID de VPC para VPC1 del paso anterior.

```
[ec2-user@cli-host ~]$ aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00273783f78bba119 --traffic-type ALL --log-destination
-type s3 --log-destination arn:aws:s3:::flowlog123456
{
    "Unsuccessful": [],
    "FlowLogIds": [
        "fl-0170cac920bac2fb9"
    ],
    "ClientToken": "A7Om7xBTJI9gMMNoayKg6TYDOcEvJY9DQOLP7kFmx/c="
}
[ec2-user@cli-host ~]$
```

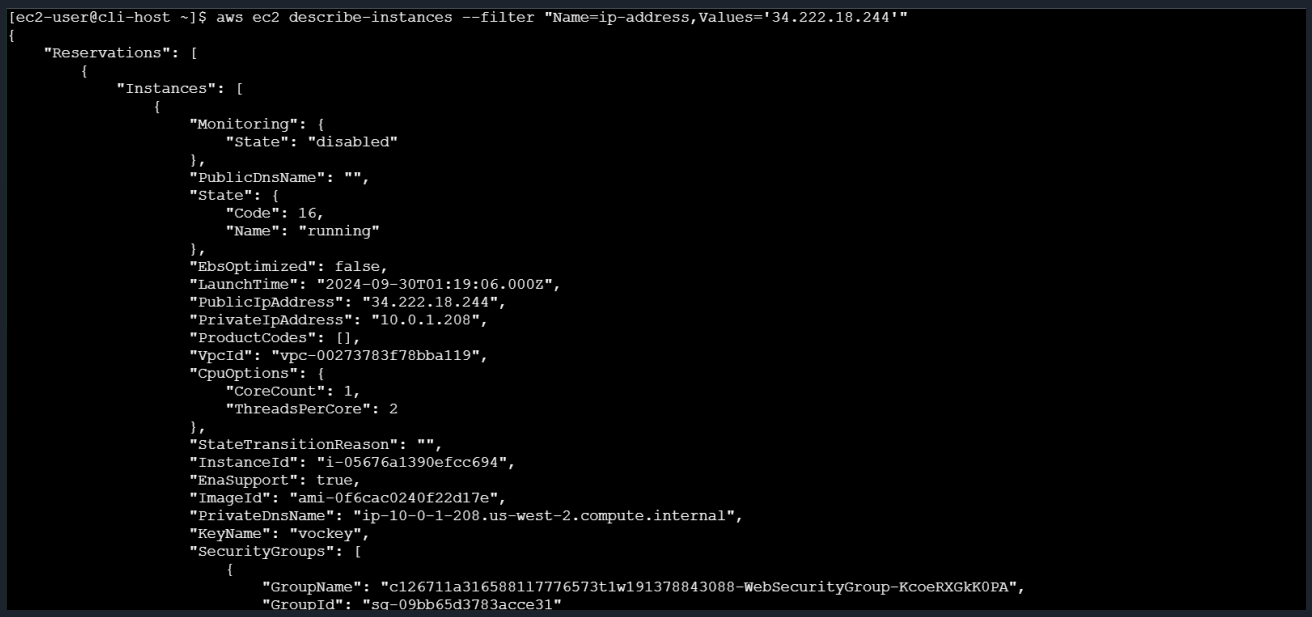
- Para confirmar que se creó el registro de flujo, ejecute el siguiente comando:

```
[ec2-user@cli-host ~]$ aws ec2 describe-flow-logs
{
    "FlowLogs": [
        {
            "LogDestinationType": "s3",
            "Tags": [],
            "ResourceId": "vpc-00273783f78bba119",
            "CreationTime": "2024-09-30T01:34:13.895Z",
            "TrafficType": "ALL",
            "FlowLogStatus": "ACTIVE",
            "LogFormat": "${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes
} ${start} ${end} ${action} ${log-status}",
            "FlowLogId": "fl-0170cac920bac2fb9",
            "MaxAggregationInterval": 600,
            "LogDestination": "arn:aws:s3:::flowlog123456",
            "DeliverLogsStatus": "SUCCESS"
        }
    ]
}
[ec2-user@cli-host ~]$
```

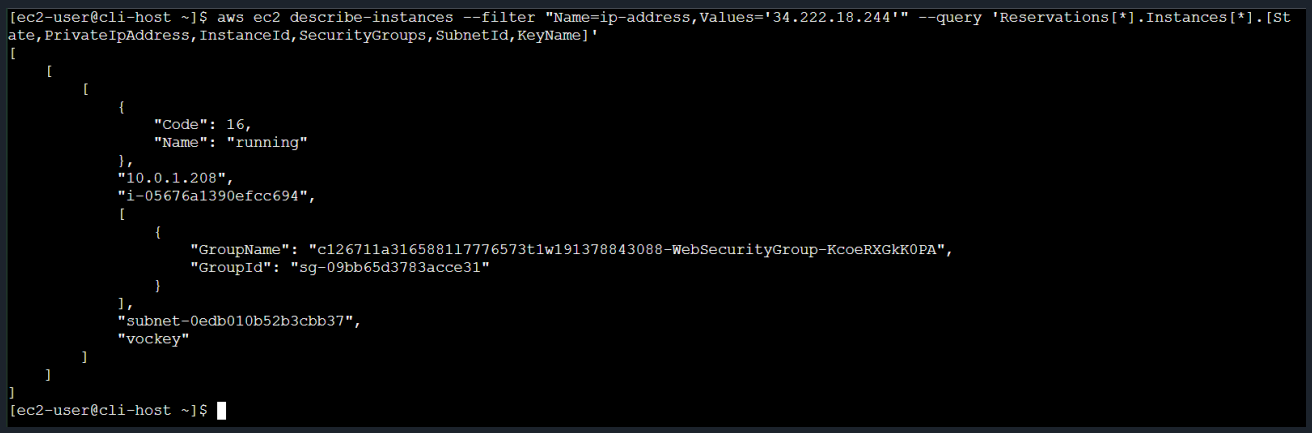
TAREA 3

En esta tarea, analizará el acceso a la instancia del servidor web y solucionará algunos problemas de red. Recuerde que la instancia del servidor web de la cafetería se ejecuta en la subred pública en VPC1. Consulte el diagrama que se encuentra al comienzo de este laboratorio para ver detalles sobre cómo se debe configurar la red.

- Desde su editor de texto, copie la dirección IP de WebServerIP y péguela en una nueva pestaña del navegador.
- Después de unos momentos, la página no se carga y recibes un mensaje que indica que no se puede acceder al sitio o que se agotó el tiempo de conexión. Este mensaje es el esperado.
- En la terminal del host de la CLI, para buscar detalles sobre la instancia del servidor web, ejecute el siguiente comando. En el comando, reemplace <WebServerIP> por la dirección WebServerIP que utilizó en los pasos anteriores:



- Para filtrar los resultados, ejecute el siguiente comando. En el comando, reemplace <WebServerIP> con la misma dirección WebServerIP que utilizó en los pasos anteriores:



- En la pestaña del navegador con la Consola de administración de AWS, en la barra de búsqueda, ingrese y elija EC2 abrir la Consola de administración de EC2.
- En el panel de navegación, seleccione Instancias.
- De la lista de instancias, seleccione la instancia de Cafe Web Server.
- Seleccione Conectar.
- En la pestaña Conectar instancia EC2, seleccione Conectar.

Failed to connect to your instance

EC2 Instance Connect is unable to connect to your instance. Ensure your instance network settings are configured correctly for EC2 Instance Connect. For more information, see EC2 Instance Connect Prerequisites at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html.

DESAFÍO 1

Has determinado que la instancia del servidor web está en ejecución, pero la página web no se carga. ¿Cuál podría ser el problema?

Desafíese a realizar su investigación utilizando únicamente el acceso programático de AWS CLI. Evite utilizar la consola de administración de AWS.

- Instalar nmap en HostCLI.

```
[ec2-user@cli-host ~]$ sudo yum install -y nmap
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                                          | 3.6 kB  00:00:00
Resolving Dependencies
--> Running transaction check
---> Package nmap.x86_64 2:6.40-19.amzn2.0.1 will be installed
--> Processing Dependency: nmap-ncat = 2:6.40-19.amzn2.0.1 for package: 2:nmap-6.40-19.amzn2.0.1.x86_64
--> Running transaction check
---> Package nmap-ncat.x86_64 2:6.40-19.amzn2.0.1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====================================================================================================================
 Package                         Arch                  Version                        Repository                Size
=====================================================================================================================
Installing:
 nmap                            x86_64                2:6.40-19.amzn2.0.1            amzn2-core               4.0 M
Installing for dependencies:
 nmap-ncat                       x86_64                2:6.40-19.amzn2.0.1            amzn2-core               204 k

Transaction Summary
=====================================================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 4.2 M
Installed size: 16 M
Downloading packages:
(1/2): nmap-ncat-6.40-19.amzn2.0.1.x86_64.rpm                                       | 204 kB  00:00:00
(2/2): nmap-6.40-19.amzn2.0.1.x86_64.rpm                                            | 4.0 MB  00:00:00
---------------------------------------------------------------------------------------------------------------------
Total                                                                      26 MB/s | 4.2 MB  00:00:00
Running transaction check
Running transaction test
```

- Nmap más la IP del servidor.

```
[ec2-user@cli-host ~]$ nmap 34.222.18.244

Starting Nmap 6.40 ( http://nmap.org ) at 2024-09-30 01:56 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
[ec2-user@cli-host ~]$
```

- Describir grupo de seguridad.

```
[ec2-user@cli-host ~]$ aws ec2 describe-security-groups
{
    "SecurityGroups": [
        {
            "IpPermissionsEgress": [
                {
                    "IpProtocol": "-1",
                    "PrefixListIds": [],
                    "IpRanges": [
                        {
                            "CidrIp": "0.0.0.0/0"
                        }
                    ],
                    "UserIdGroupPairs": [],
                    "Ipv6Ranges": []
                }
            ],
            "Description": "default VPC security group",
            "IpPermissions": [
                {
                    "IpProtocol": "-1",
                    "PrefixListIds": [],
                    "IpRanges": [],
                    "UserIdGroupPairs": [
                        {
                            "UserId": "191378843088",
                            "GroupId": "sg-05e0ebdf7d6b21cbc"
                        }
                    ],
```

- Buscar la conectividad del puerto 22.

```
[ec2-user@cli-host ~]$ aws ec2 describe-security-groups --group-ids 'sg-09bb65d3783acce31'
{
    "SecurityGroups": [
        {
            "IpPermissionsEgress": [
                {
                    "IpProtocol": "-1",
                    "PrefixListIds": [],
                    "IpRanges": [
                        {
                            "CidrIp": "0.0.0.0/0"
                        }
                    ],
                    "UserIdGroupPairs": [],
                    "Ipv6Ranges": []
                }
            ],
            "Description": "Enable HTTP access",
            "Tags": [
                {
                    "Value": "arn:aws:cloudformation:us-west-2:191378843088:stack/c126711a316588117776573t1w191378843088/a0b88bf0-7ec9-11ef-9
f9d-0ac1911b680d",
                    "Key": "aws:cloudformation:stack-id"
                },
                {
                    "Value": "WebSecurityGroup",
                    "Key": "aws:cloudformation:logical-id"
                },
                {
                    "Value": "c126711a316588117776573t1w191378843088",
                    "Key": "aws:cloudformation:stack-name"
                },
                {
                    "Value": "WebSecurityGroup",
```

- Configuración de la tabla de rutas

```
[ec2-user@cli-host ~]$ aws ec2 describe-route-tables  --route-table-ids 'rtb-07073b6d43b2d6cfc' --filter "Name=association.subnet-id,Values='
subnet-0edb010b52b3cbb37'"
{
    "RouteTables": [
        {
            "Associations": [
                {
                    "SubnetId": "subnet-0edb010b52b3cbb37",
                    "AssociationState": {
                        "State": "associated"
                    },
                    "RouteTableAssociationId": "rtbassoc-0d2f49b980367d21a",
                    "Main": false,
                    "RouteTableId": "rtb-07073b6d43b2d6cfc"
                }
            ],
            "RouteTableId": "rtb-07073b6d43b2d6cfc",
            "VpcId": "vpc-00273783f78bba119",
            "PropagatingVgws": [],
            "Tags": [
                {
                    "Value": "VPC1 Public Route Table",
                    "Key": "Name"
                },
                {
                    "Value": "arn:aws:cloudformation:us-west-2:191378843088:stack/c126711a316588117776573t1w191378843088/a0b88bf0-7ec9-11ef-9
f9d-0ac1911b680d",
                    "Key": "aws:cloudformation:stack-id"
                },
                {
                    "Value": "VPC1PublicRouteTable",
                    "Key": "aws:cloudformation:logical-id"
                },
                {
```

- Definir nueva ruta.

```
[ec2-user@cli-host ~]$ aws ec2 create-route --route-table-id 'rtb-07073b6d43b2d6cfc' --gateway-id  'igw-0b093c3c30a18ed04' --destination-cidr
-block '0.0.0.0/0'
{
    "Return": true
}
[ec2-user@cli-host ~]$
```

- Recargar la página web.

DESAFÍO 2

Ahora que resolvió el problema de acceso web, intente conectarse a la instancia del servidor web mediante EC2 instance Connect.

Este intento también falla. Aparece en el navegador un mensaje de error similar al que recibiste anteriormente. Nuevamente, este comportamiento es el esperado.

¿Cuál podría ser el problema restante?

Ya ha verificado que el servidor web está en ejecución. Ha creado correctamente una entrada en la tabla de rutas para conectar la subred donde se ejecuta la instancia del servidor web a Internet. También ha verificado que el grupo de seguridad permite conexiones en el puerto 22, que es el puerto SSH predeterminado.

- Verifique la configuración de la lista de control de acceso a la red (ACL de red) para la ACL de red que está asociada con la subred donde se ejecuta la instancia.

```
[ec2-user@cli-host ~]$ aws ec2 describe-network-acls --filter "Name=association.subnet-id,Values='subnet-0edb010b52b3cbb37'" --query 'NetworkAcls[*].[NetworkAclId,Entries]'
[
    [
        "acl-0957af13c0bc15b53",
        [
            {
                "RuleNumber": 100,
                "Protocol": "-1",
                "Egress": true,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "allow"
            },
            {
                "RuleNumber": 32767,
                "Protocol": "-1",
                "Egress": true,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "deny"
            },
            {
                "RuleNumber": 40,
                "Protocol": "6",
                "PortRange": {
                    "To": 22,
                    "From": 22
                },
                "Egress": false,
                "RuleAction": "deny",
                "CidrBlock": "0.0.0.0/0"
            },
            {
                "RuleNumber": 100,
                "Protocol": "-1",
```

- Eliminar cualquier entrada de ACL de red que pueda estar causando un problema.

```
[ec2-user@cli-host ~]$ aws ec2 delete-network-acl-entry --network-acl-id 'acl-0957af13c0bc15b53' --ingress --rule-number 40
[ec2-user@cli-host ~]$
```

- Reinterar la conexión a la instancias cafewebeserver.

```
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@web-server ~]$ hostname
web-server
[ec2-user@web-server ~]$
```

TAREA 4

Ha resuelto los problemas de red. Al hacerlo, creó algunas entradas útiles en los registros de flujo que creó al crear los registros de flujo de VPC al comienzo de este laboratorio.

En esta tarea final, consulta los registros de flujo para observar las actividades que capturan.

- En la ventana de terminal del host CLI, para crear un directorio local donde pueda descargar los archivos de registro de flujo, ejecute el siguiente comando:

```
[ec2-user@cli-host ~]$ mkdir flowlogs
[ec2-user@cli-host ~]$
```

- Para cambiar el directorio al nuevo directorio, ejecute el siguiente comando:

```
[ec2-user@cli-host ~]$ cd flowlogs
[ec2-user@cli-host flowlogs]$
```

- Para enumerar los depósitos S3 y recordar el nombre del depósito, ejecute el siguiente comando:

```
[ec2-user@cli-host flowlogs]$ aws s3 ls
2024-09-30 01:34:15 flowlog123456
[ec2-user@cli-host flowlogs]$
```

- Para descargar los registros de flujo, ejecute el siguiente comando. En el comando, reemplace < flowlog###### > con

el nombre del depósito que utilizó anteriormente en el laboratorio:

```
[ec2-user@cli-host flowlogs]$ aws s3 cp s3://flowlog123456/ . --recursive
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0135Z_1cf6ff51.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0135Z_1cf6ff51.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0135Z_05e1ffb0.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0135Z_05e1ffb0.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0145Z_65491989.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0145Z_65491989.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0200Z_223a84de.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0200Z_223a84de.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0140Z_3b5aa994.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0140Z_3b5aa994.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0145Z_4e31bd05.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0145Z_4e31bd05.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0155Z_3a41ed64.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0155Z_3a41ed64.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0200Z_9ca3c317.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0200Z_9ca3c317.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0150Z_ee3aaa9d.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
_20240930T0150Z_ee3aaa9d.log.gz
download: s3://flowlog123456/AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20
240930T0150Z_81095ecb.log.gz to AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9
```

- Para llegar al subdirectorio requerido, ejecute el siguiente comando cd. En el comando, reemplace < AWSLogs/AccountID/vpcflowlogs/us-west-2/yyyy/mm/dd/ > con el subdirectorio del resultado del comando anterior:

```
[ec2-user@cli-host flowlogs]$ cd AWSLogs/191378843088/vpcflowlogs/us-west-2/2024/09/30/
[ec2-user@cli-host 30]$
```

- Para ver todos los archivos de registro descargados, ejecute el ls comando. Los registros se encuentran en un subdirectorio AWSLogs/ < AccountID > /vpcflowlogs/ < region > /yyyy/mm/dd.

```
[ec2-user@cli-host 30]$ ls
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0135Z_05e1ffb0.log.gz
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0135Z_1cf6ff51.log.gz
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0140Z_3b5aa994.log.gz
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0140Z_93f8b2f5.log.gz
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0145Z_4e31bd05.log.gz
```

- Para extraer los registros, ejecute el siguiente comando:

```
[ec2-user@cli-host 30]$ gunzip *.gz
[ec2-user@cli-host 30]$
```

- Ejecute el ls comando nuevamente.

```
[ec2-user@cli-host 30]$ ls
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0135Z_05e1ffb0.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0135Z_1cf6ff51.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0140Z_3b5aa994.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0140Z_93f8b2f5.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0145Z_4e31bd05.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0145Z_65491989.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0150Z_81095ecb.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0150Z_ee3aaa9d.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0155Z_3a41ed64.log
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0155Z_ee45fde4.log
```

- Copie uno de los nombres de archivo que devolvió el comando ls que ejecutó en los pasos anteriores.
- En la ventana de terminal, ejecute el siguiente comando. En el comando, reemplace < nombre de archivo > por el nombre de archivo que copió en el paso anterior.

```
[ec2-user@cli-host 30]$ head 191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0135Z_05e1ffb0.log
version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status
2 191378843088 eni-0133cc24d6e146174 167.94.145.23 10.0.1.108 46889 41795 6 1 60 1727660268 1727660295 REJECT OK
2 191378843088 eni-0133cc24d6e146174 13.91.165.212 10.0.1.108 41678 49152 6 1 40 1727660268 1727660295 REJECT OK
2 191378843088 eni-0133cc24d6e146174 94.102.49.148 10.0.1.108 45626 32593 6 1 44 1727660268 1727660295 REJECT OK
2 191378843088 eni-0133cc24d6e146174 103.102.230.4 10.0.1.108 53038 8728 6 1 40 1727660268 1727660295 REJECT OK
2 191378843088 eni-0133cc24d6e146174 35.203.210.92 10.0.1.108 56914 28140 6 1 44 1727660268 1727660295 REJECT OK
2 191378843088 eni-0133cc24d6e146174 45.84.89.2 10.0.1.108 63092 3690 6 1 52 1727660268 1727660295 REJECT OK
2 191378843088 eni-0351f41827ae953e8 35.203.210.120 10.0.1.208 54997 22350 6 1 44 1727660270 1727660298 REJECT OK
2 191378843088 eni-0351f41827ae953e8 162.216.149.141 10.0.1.208 50253 8100 6 1 44 1727660270 1727660298 REJECT OK
2 191378843088 eni-0351f41827ae953e8 162.216.149.155 10.0.1.208 54731 65522 6 1 44 1727660270 1727660298 REJECT OK
[ec2-user@cli-host 30]$
```

- Para buscar cada archivo de registro en el directorio actual y devolver líneas que contengan la palabra REJECT, ejecute el siguiente comando:

```
.0.1.108 51585 189 6 1 44 1727665614 1727665629 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:37:2 191378843088 eni-0133cc24d6e146174 79.110.62.245 10.
0.1.108 45317 24794 6 1 40 1727665614 1727665629 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:38:2 191378843088 eni-0133cc24d6e146174 147.185.133.18 10
.0.1.108 56146 22085 6 1 44 1727665614 1727665629 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:39:2 191378843088 eni-0133cc24d6e146174 47.106.178.136 10
.0.1.108 48776 6379 6 1 60 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:41:2 191378843088 eni-0133cc24d6e146174 207.90.244.4 10.0
.1.108 30991 8554 6 1 44 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:42:2 191378843088 eni-0133cc24d6e146174 147.185.133.166 1
0.0.1.108 53167 7788 6 1 44 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:43:2 191378843088 eni-0133cc24d6e146174 162.216.150.34 10
.0.1.108 56876 6789 6 1 44 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:44:2 191378843088 eni-0133cc24d6e146174 94.255.233.39 10.
0.1.108 28187 23 6 1 40 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:45:2 191378843088 eni-0133cc24d6e146174 162.216.149.32 10
.0.1.108 52770 16363 6 1 44 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:46:2 191378843088 eni-0133cc24d6e146174 185.242.226.27 10
.0.1.108 54355 139 6 1 40 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:47:2 191378843088 eni-0133cc24d6e146174 162.216.149.162 1
0.0.1.108 54448 5518 6 1 44 1727665577 1727665603 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:50:2 191378843088 eni-0351f41827ae953e8 162.216.149.71 10
.0.1.208 55694 9606 6 1 44 1727665582 1727665597 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:51:2 191378843088 eni-0351f41827ae953e8 147.185.133.184 1
0.0.1.208 53977 47000 6 1 44 1727665582 1727665597 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:52:2 191378843088 eni-0351f41827ae953e8 35.203.211.223 10
.0.1.208 50734 3100 6 1 44 1727665582 1727665597 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:54:2 191378843088 eni-0351f41827ae953e8 162.216.149.106 1
0.0.1.208 50210 9474 6 1 44 1727665615 1727665629 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:55:2 191378843088 eni-0351f41827ae953e8 103.102.230.5 10.
0.1.208 51496 8728 6 1 40 1727665615 1727665629 REJECT OK
191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:56:2 191378843088 eni-0351f41827ae953e8 147.185.133.153 1
0.0.1.208 52774 1902 17 1 125 1727665615 1727665629 REJECT OK
[ec2-user@cli-host 30]$
```

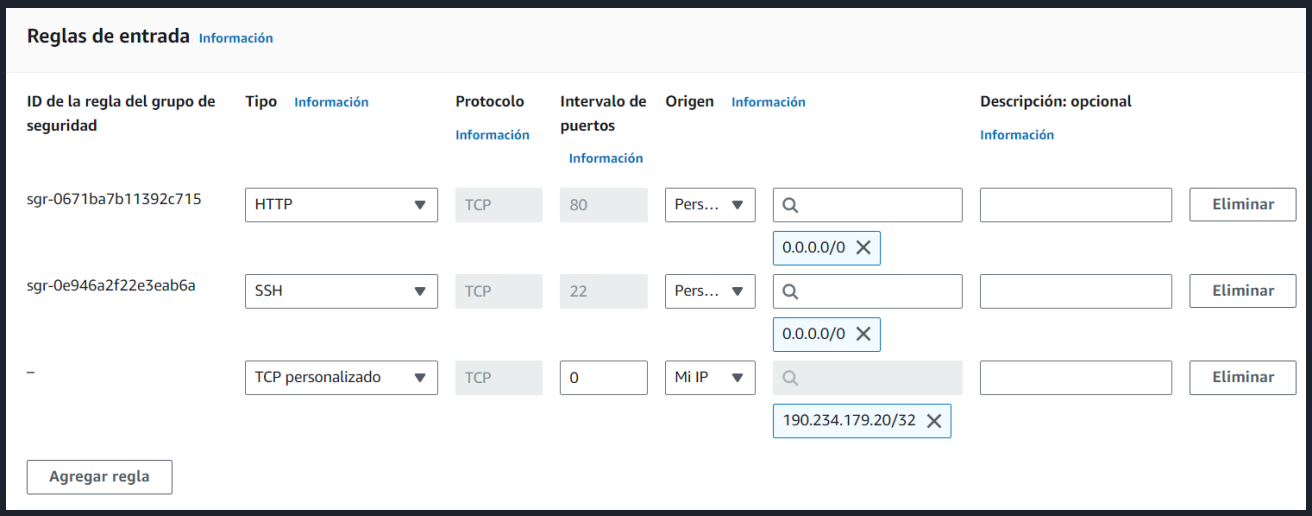
- Para saber cuántos registros se devolvieron, ejecute el siguiente comando:

```
[ec2-user@cli-host 30]$ grep  -rn REJECT . | wc  -l
3123
[ec2-user@cli-host 30]$
```

- Para refinar su búsqueda buscando solo líneas que contengan 22 (que es el número de puerto donde intentó conectarse al servidor web cuando el acceso estaba bloqueado), ejecute el siguiente comando:

```
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0350Z_0d4a44ed.log:84:2 191378843088 eni-0351f41827ae953e8 206.168.35.128
10.0.1.208 41331 52200 6 1 60 1727668282 1727668308 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0350Z_0d4a44ed.log:105:2 191378843088 eni-0133cc24d6e146174 205.210.31.131
 10.0.1.108 52269 5985 6 1 44 1727668306 1727668336 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0350Z_0d4a44ed.log:113:2 191378843088 eni-0351f41827ae953e8 80.75.212.9 10
.0.1.208 59474 22954 6 1 40 1727668317 1727668336 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0350Z_0d4a44ed.log:120:2 191378843088 eni-0351f41827ae953e8 147.185.132.16
0 10.0.1.208 54489 22998 6 1 44 1727668317 1727668336 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0350Z_0d4a44ed.log:132:2 191378843088 eni-0133cc24d6e146174 4.151.229.42 1
0.0.1.108 36271 3351 6 1 40 1727668343 1727668363 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:3:2 191378843088 eni-0351f41827ae953e8 45.14.226.14 10.
0.1.208 43134 11211 6 1 40 1727665499 1727665518 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:9:2 191378843088 eni-0133cc24d6e146174 79.110.62.147 10
.0.1.108 47222 29791 6 1 40 1727665488 1727665508 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:15:2 191378843088 eni-0133cc24d6e146174 147.185.133.49
10.0.1.108 52235 9921 6 1 44 1727665549 1727665572 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:29:2 191378843088 eni-0351f41827ae953e8 185.16.39.29 10
.0.1.208 25685 37020 17 1 122 1727665550 1727665580 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:30:2 191378843088 eni-0351f41827ae953e8 185.242.226.27
10.0.1.208 60830 139 6 1 40 1727665550 1727665580 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:33:2 191378843088 eni-0351f41827ae953e8 83.222.190.122
10.0.1.208 56372 6756 6 1 40 1727665550 1727665580 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:35:2 191378843088 eni-0351f41827ae953e8 162.216.150.248
 10.0.1.208 52330 22445 6 1 44 1727665550 1727665580 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:38:2 191378843088 eni-0133cc24d6e146174 147.185.133.18
10.0.1.108 56146 22085 6 1 44 1727665614 1727665629 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:46:2 191378843088 eni-0133cc24d6e146174 185.242.226.27
10.0.1.108 54355 139 6 1 40 1727665577 1727665603 REJECT OK
./191378843088_vpcflowlogs_us-west-2_fl-0170cac920bac2fb9_20240930T0305Z_c2a7c94d.log:52:2 191378843088 eni-0351f41827ae953e8 35.203.211.223
10.0.1.208 50734 3100 6 1 44 1727665582 1727665597 REJECT OK
```

- En la consola de administración de AWS, vaya al servicio Amazon EC2 en la misma región donde se ejecutan sus instancias EC2.
- Seleccione Grupos de seguridad.
- Seleccione el enlace para WebSecurityGroup y luego elija la pestaña Reglas de entrada.
- Seleccione Editar reglas de entrada y luego seleccione Agregar regla.
- En la tercera fila que acabas de crear, para Origen, elige Mi IP.
- Copie la dirección IP del bloque de enrutamiento entre dominios sin clases (CIDR) que se completa automáticamente (terminará en /32) y péguela en un editor de texto. Copie solo la dirección IP, no el sufijo /32.



- Seleccione Cancelar.
- En la sesión de terminal del host de CLI, ejecute la siguiente consulta refinada en los registros de flujo. En el siguiente comando, reemplace <ip-address> con la dirección IP del bloque CIDR que copió en los pasos anteriores:

```
[ec2-user@cli-host 30]$ grep  -rn  22 . | grep REJECT | grep 190.234.179.20
[ec2-user@cli-host 30]$
```

- Para confirmar que el ID de la interfaz de red que se registra en el registro de flujo coincide con la interfaz de red que se asigna a la instancia del servidor web (como parte de la interfaz de red), ejecute el siguiente comando. En el comando, reemplace <WebServerIP> con la dirección IP del editor de texto:

```
[ec2-user@cli-host 30]$ grep  -rn  22 . | grep REJECT | grep 190.234.179.20
[ec2-user@cli-host 30]$ aws ec2 describe-network-interfaces --filters "Name=association.public-ip,Values='190.234.179.20'" --query 'NetworkInterfaces[*].[NetworkInterfaceId,Association.PublicIp]'
[]
[ec2-user@cli-host 30]$
```

- Para traducir una de las marcas de tiempo a un formato legible para humanos, ejecute el date -d @comando correspondiente a una de las marcas de tiempo capturadas de uno de los resultados de RECHAZO filtrados. Debería

indicar una hora de hoy que corresponda a cuando estaba trabajando en este laboratorio.

```
[ec2-user@cli-host 30]$ date -d @1554496931
Fri Apr  5 20:42:11 UTC 2019
[ec2-user@cli-host 30]$
```

- Para comparar el resultado con la hora actual, ejecute el siguiente comando:

```
[ec2-user@cli-host 30]$ date
Mon Sep 30 04:13:04 UTC 2024
[ec2-user@cli-host 30]$
```